(12) **EUROPEAN PATENT APPLICATION**

(72) Inventor: Herbert, Raymond John
Leigh-on-Sea, Essex, SS9 3PP (GB)

(74) Representative:
Loughrey, Richard Vivian Patrick et al
HUGHES CLARK & CO
114-118 Southampton Row
London WC1B 5AA (GB)

(54) **Secure communication system**

(57) A secure communication system for transmission of messages utilises postage meters (10) as terminals of the system. The postage meters include means (13) for input of postage amount, an encryptor (26) to encrypt postage information to be printed by a printer (21) of the meter. The input means are used for input of a message, the encryptor encrypts the message with a key unique for an intended recipient terminal and the printer prints the encrypted message on a mail item (20). The terminals also are provided with reading means (31; 32) to read a received encrypted message (30) and the encryption means (26) is utilised to decrypt the received encrypted message using the unique key of the recipient terminal.
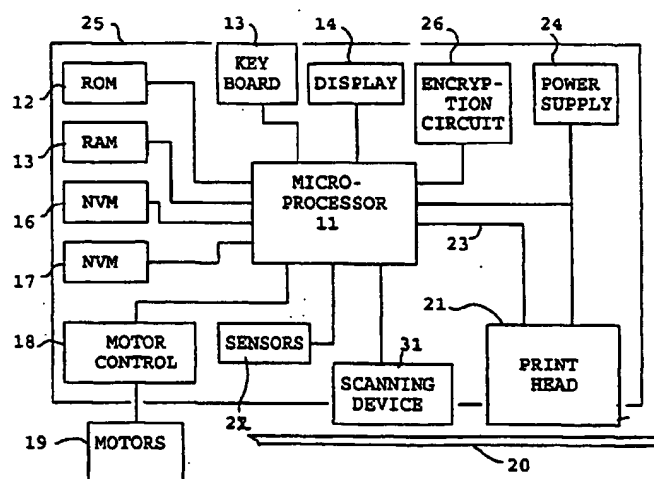
FIG 1

Description

This invention relates to a system for secure communication of messages from an originator of a message to an intended recipient of the message.

In systems for applying postage indicia to mail items it has been proposed to include encrypted information in the imprint of the postage indicia in order to provide security in respect of the postage indicia. The information which is encrypted relates to the postage meter system utilised to print the indicia so as to identify the mailer and also relates to postage information, for example the amount of postage charge applicable to the mail item and for which accounting has been effected. The encrypted information may be printed as alphanumeric characters but it has also been proposed to print the encrypted information in the form of a so-called 2D code comprising an array of binary elements of first and second characteristics, for example black and white.

According to the invention a secure communication system includes a sender postage metering terminal and a plurality of recipient postage metering terminals, each terminal comprising input means for input of a postage charge; encryption means for encrypting postage information; printing means for printing a postage indicium including said encrypted postage information on a mail item; wherein the input means is operable to input a message, intended for receipt by a designated one of the recipient terminals, to said encryption means; said encryption means being operable to encrypt said message using a key unique to the designated recipient terminal; and each terminal including means for input of a received encrypted message to the encryption means and the encryption means being operable to use a key unique to that terminal to decrypt the encrypted message.

An embodiment of the invention will now be described with reference to the drawings in which:-

Figure 1 is a block diagram of a postage meter for use as a terminal in a secure message transmission system, and
Figure 2 illustrates a hand held scanning device connected to the postage meter.

Referring first to Figure 1 of the drawings, a postage meter 10 includes electronic accounting and control means comprising a micro-processor 11 operating under program routines stored in a read only memory (ROM) 12. A keyboard 13 is provided for input of commands and data by a user and a display 14 is provided to enable display of information to the user. A random access memory (RAM) 13 is provided for use as a working store for storage of temporary data during operation of the postage meter. Non-volatile duplicated memories 16, 17 are provided for the storage of critical data relating to use of the postage meter and which is required to be retained even when the postage meter is not powered. The microprocessor 11 carries out accounting functions in relation to use of the postage meter for franking mail items with postage charges applicable to handling of the mail items by the postal authority or another carrier. Accounting data relating to use of the postage meter for printing franking impressions representing postage charges for mail items and any other critical data to be retained is stored in the non-volatile memories 16, 17. The accounting data includes a value of credit available for use by the meter in franking mail items, an accumulated total of value used by the meter in franking mail items, a count of the number of mail items franked by the meter and a count of the number of mail items franked with a postage charge in excess of a predetermined value. The value of credit is stored in a descending credit register, the accumulated total value is stored in an ascending tote register, the count of items is stored in an items register and the count of items franked with a postage charge in excess of a predetermined value is stored in a large items register. As is well known in the postage meter art, each of the registers referred to hereinbefore for storing accounting data is replicated in order to enable integrity of the accounting data to be maintained even in the event of a fault or termination of power to the meter during a franking operation. Two replications of each of the registers are provided in each of the memory devices 16, 17.

A motor controller 18 is controlled by the microprocessor 10 to control operation of motors 19 driving feeding means (not shown) for feeding a mail item 20 past a digital print head 21. The digital print head 21 may be a thermal print head including selectively energisable thermal printing elements. Sensors 22 are provided to sense and monitor feeding of the mail item. The sensors provide signals to the microprocessor to enable the microprocessor to control feeding of the mail item and to selectively energise the thermal print elements of the print head at appropriate times as the mail item is fed past the print head. As the mail item is fed past the thermal printing elements of the print head 21 during a printing operation, the microprocessor outputs on line 23, in each of a series of printing cycles, print data signals selecting those ones of the printing elements which are to be energised in each respective printing cycle. A pulse of electrical power is supplied to the selected thermal printing elements from a power source 24.

The thermal printing elements are disposed in a line extending transversely to the direction in which the mail item is fed. Energisation of selected thermal printing elements of the print head in a printing cycle causes the thermal transfer selected areas of ink from an ink ribbon and repeated selection and energisation of selected printing elements in the series of printing cycles results in printing of dots in required positions of a corresponding series of columns spaced along the mail item in the direction of feeding of the item. Accordingly a complete printed impression is built up in a column by column manner in the series of printing cycles of

a printing operation. It is to be understood that although the postage meter is described hereinbefore as including a thermal printer for printing franking impressions on mail items, the postage meter may include other types of digital printing device such as , for example, impact dot matrix, ink jet and laser.

It will be appreciated that, as is well known in the postage meter art, the postage meter must operate in a secure manner and be protected from attempts to use the meter fraudulently for example by utilising the postage meter to print franking impressions on mail items for which no corresponding postage charge has been accounted for by the accounting means. Accordingly those parts of the postage meter required to be secured against unauthorised tampering are housed in a secure housing 25.

In order to provide security in the printed postage indicium, the postage meter is provided with means to encrypt information. In the present embodiment as illustrated in figure 1, the encryption means is an encryption circuit 26 connected to the microprocessor 11. However if desired encryption of the information may be effected by the microprocessor 11 operating under a software routine. postage information, which includes the postage amount and may include other data as well, is encrypted by the encryption circuit 26, or by the microprocessor 11, and the resulting encrypted information is included as part of the information included in the postage indicium printed by the print head.

When carrying out a franking operation, postage information including a postage charge to be applied to the mail item 20 is input to the microprocessor 11 by means of a keyboard 13. The microprocessor 11 carries out accounting functions in respect of the postage charge and the encryption circuit 26 operates on the postage information to generate encrypted information. The encrypted information is input to the microprocessor which then outputs print signals to the print head to cause the print head to print a postage indicium 27 (see Figure 2) including the postage information and the encrypted information on a mail item. The postage information may be printed in visually readable form 28 and also in machine readable code form 29, for example 2D code comprising an array of pixels representing the information.

In accordance wit the present invention it is proposed to utilise the postage meter 10 to print additional information 30 comprising a message encrypted in the form of a 2D code and to enable the reading and decrypting of this message by use of a recipient's postage meter. The message 30 may be printed on the exterior of the mail item 20 and may be printed in the same printing operation as that in which the postage indicium 27 is printed or the message may be printed on an insert placed inside an envelope. The message is encrypted utilising the encryption circuit 26 in a manner to ensure that it is intelligible only to an intended recipient. Accordingly the message is encrypted using data

unique to the recipient's postage meter and this data may for example comprise a serial number of the meter or a security key. In addition, or alternatively, a secret key may be used in the encryption of the additional information. The secret key would be a key known only to both the sender and the intended recipient of the information and use of this key would be agreed by the sender and intended recipient prior to sending the message.

The postage meter, as shown in Figure 1, is provided with a scanning device 31 housed in the housing 25. The scanning device 31 is connected to the microprocessor 11 and is operable to scan information in 2D code form on a received mail item 20. The item 20 carries the postage indicium which may include both the visually readable portion 28 and a portion 29 in 2D code. In addition the item carries the encrypted message 30 in 2D code. When the item is received the message on the item is scanned by the scanning device 31 and electrical scanning signals resulting from the scanning of the item are input to the microprocessor 11. The microprocessor inputs these scanning signals to the encryption circuit 26 which is operable to utilise data unique to that recipient terminal, for example the security key or the serial number of the meter, to decrypt the scanned encrypted information and thereby produce the message in non-encrypted form. The encryption circuit outputs the decrypted message to the microprocessor where it may be displayed on the display 14 or may be output to the print head 21 to produce a printed copy of the message. It will be appreciated that if the message is received by a person other than the intended recipient the message will not be intelligible to that person in its encrypted form and the message can not be decrypted without the key known to the intended recipient.

The scanning device may be a device 14 housed in the housing of the postage meter as shown in Figure 1 or may be a hand held device 32 connected by a flexible cable 33 to the postage meter 10 as shown in Figure 2.

As mentioned hereinbefore, instead of providing an encryption circuit to encrypt postage information, encryption of the postage information may be effected by the microprocessor operating under the control of a software program routine. It is to be understood that information to be included in a secure message likewise may be encrypted by the microprocessor and a received message be decrypted by the microprocessor operating under a software routine.

By printing the encrypted message in 2D code relatively high density of the information contained in the message may be attained. Accordingly a relatively long message which in plain text alpha characters would occupy more than one page could be contained within 2D code printed on an item the size of a conventional postcard.

While it may be convenient to use the same code for the printing of the postage indicium 29 and the mes-

sage 30, the code used for printing the message 30 may be different from the code used to print the postage indicium 29. For example, the postage indicium may be printed using a code known as PDF417 while the message may be printed using a Datamatrix code. If obtaining high density in printing of the message is not required, the encrypted message may be printed in alphanumeric characters. An encrypted message printed in the form of alphanumeric characters could be scanned by the scanning device 31 or 32 and the microprocessor may be operated under character recognition software to generate signals representing the alphanumeric characters for input to the encryption circuit or the alphanumeric characters of the printed encrypted message may be input by an operator using the keyboard 13.

The secure message transmission system described hereinbefore may be used for internal mail within a company where each department has a terminal as shown in the drawing comprising a personal computer to which is connected a secure unit, a printer and a scanning device.

The item of mail would be addressed, by a visually readable destination address, to an intended recipient department or person and the item would bear a message printed in encrypted form for that department or person. Upon receipt of the item, the message would be input to the computer either by scanning or, if the encrypted message is printed in alphanumeric characters, by input on the keyboard. An operator in the intended recipient department, or the intended recipient person, then enters identification information by means of the keyboard, by means of a card read by the scanning device or by a smart card coupled via reading means to the computer. The identification information input to the computer consists of or includes a key for use by the decryption circuit of the secure module to decrypt the encrypted message.

If desired, a database of keys for use in encryption and decryption of information may be located at a postal authority centre for use by operators of the franking machine message transmission terminals. Access to the database may be provided by the same communication means utilised for other communications of the franking machine and postal authority centre for example as used when resetting credit in the franking machines.

Hereinbefore, the terminal for transmission and reception of a secure message has been described as a dedicated postage meter. However postage metering systems are known comprising a secure postage metering unit connected to a personal computer. The secure postage metering unit performs the secure accounting functions and encryption functions of a dedicated postage meter but does not include the printer of a dedicated postage meter. Accordingly, if desired the terminal may comprise a secure postage metering unit connected to a personal computer.

Postage meters operating in a pre-payment mode include non-volatile registers storing values of credit available for use in franking operations. In the same manner, the secure postage metering unit includes a non-volatile register storing a value of credit. Since the message transmitted from one terminal is to a designated recipient, the secure message transmission system described hereinbefore may be utilised to transfer value stored in the non-volatile register of one terminal to a non-volatile register of a designated terminal.

Claims

1. A secure communication system characterised by a sender postage metering terminal (10) and a plurality of recipient postage metering terminals (10), each terminal (10) comprising input means (13) for input of a postage charge; encryption means (26) for encrypting postage information; printing means (21) for printing a postage indicium (27) including said encrypted postage information (29) on a mail item (20); wherein the input means (13) of the sender terminal is operable to input a message, intended for receipt by a designated one of the recipient terminals, to the encryption means (26) of the sender terminal; said encryption means of the sender terminal being operable to encrypt said message using a key unique to the designated recipient terminal; and each recipient terminal including means (31) for input of a received encrypted message (30) to the encryption means (26) of the recipient terminal; and the encryption means of the designated recipient terminal being operable to use a key unique to that terminal to decrypt the encrypted message.

2. A secure communication system as claimed in claim 1 wherein the printing means (21) of the sender terminal is operable to print the encrypted message (30) on a mail item (20) and wherein the input means of the recipient terminals includes means (31; 32) to read the printed encrypted message from the mail item (20).

3. A secure communication system as claimed in claim 1 or 2 wherein the printing means (21) of the sender terminal is operable to print the encrypted message in the form of a 2D code.

4. A secure communication system as claimed in any preceding claim wherein the key unique to the recipient terminal comprises an identification number of the designated terminal.

5. A secure communication system as claimed in any preceding claim wherein the key unique to the recipient terminal comprises a secure secret key.

6. A secure communication system as claimed in any preceding claim wherein the printing means (21) of the recipient terminal is operable to print the decryption of the encrypted message.

5

7. A secure communication means as claimed in any preceding claim wherein the recipient terminal includes display means (14) operable to display the decryption of the encrypted message.

10

8. A secure communication system as claimed in claim 2 wherein the means for reading the encrypted message includes a hand-held scanner (32) connected to the recipient terminal.

15

9. A secure communication system as claimed in any preceding claim wherein the terminals each comprise a secure postage metering unit connected to a computer and a printer connected to the computer.
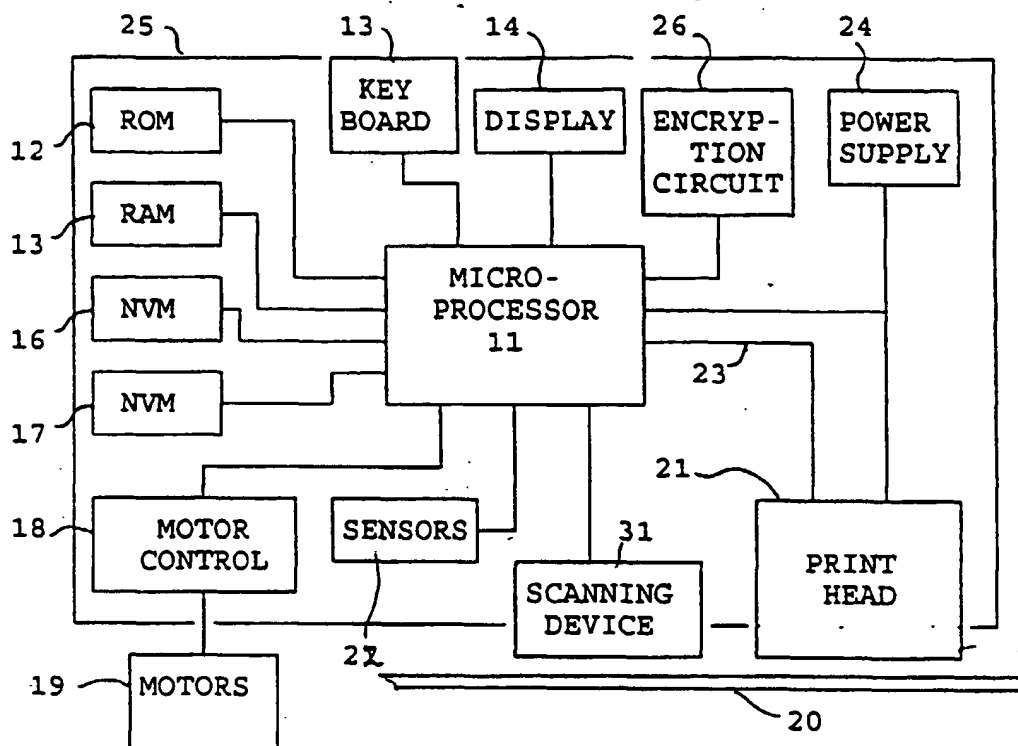
20

25

30

35

40

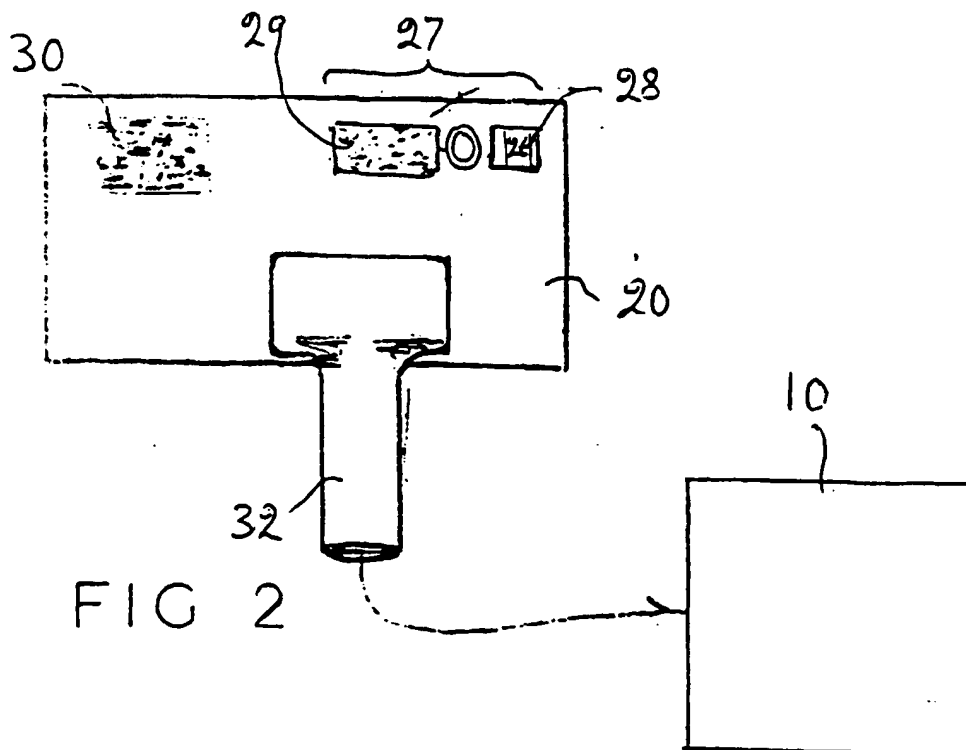*45*

50

55

25

13

14

26

24

KEY
BOARD

DISPLAY

ENCRYP-
TION
CIRCUIT

POWER
SUPPLY

ROM

12

RAM

13

NVM

16

MICRO-
PROCESSOR
11

NVM

17

23

21

MOTOR
CONTROL

18

SENSORS

31

PRINT
HEAD

22

SCANNING
DEVICE

19

MOTORS

20

FIG 1

30

29

27

28

20

10

32

FIG 2

EUROPEAN PATENT APPLICATION

(72) Inventor: **Herbert, Raymond John**
Leigh-on-Sea, Essex, SS9 3PP (GB)

(74) Representative:
**Loughrey, Richard Vivian Patrick et al
HUGHES CLARK & CO
114-118 Southampton Row
London WC1B 5AA (GB)**

(54) Secure communication system

(57) A secure communication system for transmission of messages utilises postage meters (10) as terminals of the system. The postage meters include means (13) for input of postage amount, an encryptor (26) to encrypt postage information to be printed by a printer (21) of the meter. The input means are used for input of a message, the encryptor encrypts the message with a key unique for an intended recipient terminal and the printer prints the encrypted message on a mail item (20). The terminals also are provided with reading means (31; 32) to read a received encrypted message (30) and the encryption means (26) is utilised to decrypt the received encrypted message using the unique key of the recipient terminal.
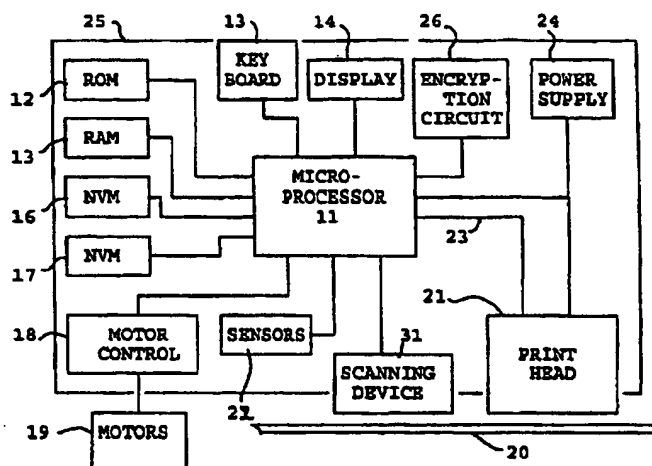
FIG 1

European Patent
Office

EUROPEAN SEARCH REPORT

Application Number

EP 98 30 0602

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
A	EP 0 733 998 A (PITNEY BOWES) 25 September 1996 (1996-09-25) * abstract * * column 3, line 3 - line 55 * * figures 1-4 *	1-9	G07B17/00 H04L9/00
A	US 5 159 635 A (WANG YNJIUM P) 27 October 1992 (1992-10-27) * abstract * * column 2, line 5 - line 58 * * column 3, line 12 - line 18 * * figures 1-6 *	1-9	
A	US 5 245 655 A (BUEHN WILLI ET AL) 14 September 1993 (1993-09-14) * abstract * * figure 1 *	1-9	
A	EP 0 600 646 A (PITNEY BOWES) 8 June 1994 (1994-06-08) * abstract *	1-9	

TECHNICAL FIELDS SEARCHED (Int.Cl.6)

G07B
H04L
H04N

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	22 June 2000	Van Dop, E

EPO FORM 1503 03.82 (P04C01)

2

ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.

EP 98 30 0602

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report.
The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

22-06-2000

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
EP 0733998	A	25-09-1996	US	5701249 A	23-12-1997
			CA	2172460 A	24-09-1996
US 5159635	A	27-10-1992	US	5866888 A	02-02-1999
			US	5646389 A	08-07-1997
			US	5393965 A	28-02-1995
			US	5401944 A	28-03-1995
			EP	0565738 A	20-10-1993
			US	5471533 A	28-11-1995
			US	5489158 A	06-02-1996
			US	5710419 A	20-01-1998
			US	5113445 A	12-05-1992
			US	5243655 A	07-09-1993
			US	5337361 A	09-08-1994
			US	5880453 A	09-03-1999
US 5245655	A	14-09-1993	AT	119705 T	15-03-1995
			CA	2025504 A	19-03-1991
			DE	59008628 D	13-04-1995
			EP	0418742 A	27-03-1991
			ZA	9007305 A	28-08-1991
EP 0600646	A	08-06-1994	US	5388158 A	07-02-1995
			CA	2109554 A,C	21-05-1994
			JP	7005809 A	10-01-1995